



# El Mercado y la Ciberseguridad

Centros de Servicios de Medicare y Medicaid (CMS)

Centro de Información al Consumidor y Supervisión de Seguros (CCIIO)

*18 de mayo de 2022*

# Exención de responsabilidad



*La información proporcionada en este documento se ofrece solamente como resumen general de normas jurídicas técnicas. No pretende sustituir a las leyes, reglamentos u orientaciones, ni políticas formales en las que se basa. Este documento resume la política y las operaciones actuales en la fecha de su presentación. Se han proporcionado enlaces a determinados documentos fuente para mayor referencia. Invitamos a los miembros de la audiencia a consultar los estatutos, reglamentos y otros materiales interpretativos aplicables para obtener información completa y actualizada sobre los requisitos que se les aplican. El contenido de este documento no tiene carácter de ley y no pretende vincular al público de ninguna manera, a menos que se incorpore específicamente a un contrato. El único propósito de este documento es dar mayor claridad al público sobre los requisitos legales existentes.*

*Este documento en general no está pensado para su uso en los Mercados Estatales (SBM) que no utilizan HealthCare.gov para la elegibilidad e inscripción. Por favor, revise la guía en nuestra página web de recursos para agentes y corredores (<http://go.cms.gov/CCIOAB>) y en [Marketsplace.CMS.gov](http://Marketsplace.CMS.gov) para obtener más información.*

*A menos que se indique lo contrario, las referencias generales al "Mercado" en la presentación sólo incluyen los Mercados facilitados por el gobierno federal (FFM) y los Mercados estatales en la plataforma federal (SBM-FP).*

*Esta comunicación fue impresa, publicada o producida y difundida a expensas de los contribuyentes de los Estados Unidos.*

# Agenda



- 01** Cumplimiento de la normatividad
- 02** Consentimiento del consumidor
- 03** Resumen de seguridad de la información
- 04** Identificar y proteger la información personal identificable

- 05** Identificar vulneraciones a la ciberseguridad
- 06** Higiene de ciberseguridad y prevención de su vulneración
- 07** Respuesta a vulneraciones de la ciberseguridad
- 08** Solucionar vulneraciones a la ciberseguridad

# Cumplimiento de la normatividad: Recordatorios clave



- » Los agentes y corredores que participan en el Mercado deben completar todos los pasos aplicables del proceso de capacitación y el registro del Mercado antes de ayudar a los consumidores a seleccionar e inscribirse en planes de salud calificados (QHP).
- » Los agentes y corredores también deberán:
  - Proporcionar información correcta a los consumidores;
  - Aportar la información correcta del consumidor (por ejemplo, nombre y fecha de nacimiento, dirección, dirección de correo electrónico) al Mercado para verificar su identidad y solicitar la cobertura del QHP;
  - Abstenerse de realizar actividades de promoción o conductas engañosas;
  - Obtenga el consentimiento de cada cliente con el que trabaje antes de ayudarlo con la cobertura del Mercado, incluso antes de buscar una solicitud actual utilizando un sitio web aprobado de inscripción directa clásica (DE)/inscripción directa mejorada (EDE);
  - Proteja la información personal identificable de los consumidores (PII); y
  - Identifique e informe sobre actividades sospechosas o comportamientos potencialmente fraudulentos que observe en relación con el Mercado.
- » Por último, los agentes y corredores deben cumplir los requisitos federales y estatales aplicables, incluidas las normas de autorización y nombramiento, las condiciones de acceso al sistema y las disposiciones sobre conflictos de intereses y confidencialidad.

# Cumplimiento de la normatividad: Recordatorios clave



- » Las cuentas del consumidor de HealthCare.gov sólo deben tener el correo electrónico, el número de teléfono y las direcciones postales del consumidor (o de su representante legalmente autorizado).
  - Nunca ingrese su propia dirección de correo electrónico, número de teléfono o dirección postal de agente o corredor profesional en la solicitud de un consumidor. No conserve el acceso a la cuenta de HealthCare.gov de un cliente ni a la cuenta de correo electrónico asociada.
  - No debe crear ni utilizar direcciones ficticias en lugar de la dirección de correo electrónico o postal del consumidor. Como buena práctica, también debe evitar el uso de direcciones de correo electrónico desechables.
- » Asegúrese que sus clientes declaren los ingresos correctos cuando completan o actualizan la solicitud de elegibilidad. Reitere que lo mejor para ellos es informar de la estimación de ingresos más precisa, no la que maximice la cantidad de crédito fiscal para la prima a la que puedan tener derecho.
  - Presente únicamente las proyecciones de ingresos que el consumidor haya autorizado y confirmado con conocimiento de causa.
  - DEBE asegurarse de que los consumidores conozcan otros programas de asequibilidad de seguros a los que puedan optar en función de sus ingresos estimados. Si los consumidores pudieran ser candidatos a Medicaid/CHIP basándose en la información de su solicitud de elegibilidad, usted DEBERÍA remitirlos a la Agencia Estatal de Medicaid, o a otros recursos que puedan ayudarles a enrolarse en la cobertura.

# Actualizar las solicitudes de los consumidores

Los agentes y corredores sólo deben actualizar la solicitud/póliza de un consumidor por indicación de éste. Esto incluye, pero no se limita a:



Realización de una búsqueda de solicitudes de los consumidores a través de un sitio web aprobado de Classic DE/EDE.



Asistirles en la solicitud de ayuda financiera y/o en la inscripción en un QHP del Mercado, incluyendo la comprobación del estatus de su cobertura y la realización de actualizaciones a lo largo del año.



Llamar al Centro de Atención Telefónica del Mercado para preguntar sobre el estatus de la inscripción en el Mercado o hacer cambios para el consumidor.

**Nota:** Este requisito es diferente, y adicionalmente, al requisito de que los consumidores deben aportarle su consentimiento para cualquier uso o divulgación de su PII fuera del ámbito de la declaración de aviso de privacidad y de las funciones autorizadas para un agente o corredor del Mercado. +

# Documentar el consentimiento del consumidor



- » **Los CMS no especifican un formato o proceso estándar para obtener o documentar el consentimiento del consumidor, por lo que usted tiene flexibilidad para determinar cómo puede cumplir con este requisito.**
  - Aunque los CMS no facilitan un formulario, ni especifican que haya que firmarlo, puede utilizar un formulario de corredor de seguros de un emisor, o del Departamento de Seguros estatal, para cumplir este requisito.
  - Si ofrece asistencia verbal (por ejemplo, telefónica), puede obtener el consentimiento leyendo un guión que contenga, como mínimo, los elementos requeridos, y debe dejar constancia por escrito de que se ha obtenido el consentimiento previsto. Grabar estas conversaciones telefónicas es una buena práctica.
  - Adicionalmente, puede obtener el consentimiento por vía electrónica (por ejemplo, por correo electrónico o mensaje de texto) o en persona.
  - El consentimiento debe reconocer que el agente o corredor ha informado al consumidor de las funciones y responsabilidades que se aplican al papel del agente o corredor en el Mercado.
  - Un agente o corredor y cualquier tercero con el que hayan ingresado en una relación comercial deberán adherirse a los requisitos para el uso y la divulgación de toda la PII/información médica protegida (PHI) del consumidor, incluyendo toda la PII/PHI recopilada por el tercero.

## El registro del consentimiento debe incluir lo siguiente: +

- ✓ El nombre del individuo, empleador o empleado,
- ✓ La fecha en que se dio el consentimiento, y
- ✓ El nombre del agente o agentes, del corredor o de la agencia a la que se dio el consentimiento. Tenga en cuenta que podría incluir adicionalmente los nombres de los agentes o corredores, si quien ha dado su consentimiento ha autorizado a varios agentes o corredores dentro de la misma organización.

## Este consentimiento también debe indicar que el agente o corredor tiene permiso para: +

- ✓ Realizar una búsqueda de la solicitud del consumidor utilizando los sitios web aprobados de Classic DE/EDE en el Mercado;
- ✓ Ayudar a completar una solicitud de elegibilidad;
- ✓ Ayudar en la selección e inscripción en el plan; y
- ✓ Asistir en el mantenimiento continuo de la cuenta/inscripción.

# Vencimiento del consentimiento del consumidor



- » Los CMS no especifican una fecha de vencimiento automática para el consentimiento, porque podría resultar oneroso para cualquier persona que busque constantemente servicios del mismo agente/corredor o agencia tener que renovar repetidamente el consentimiento.
- » Por lo tanto, el consentimiento puede durar indefinidamente, a menos que el individuo, el empresario o el empleado lo revoquen. Como buena práctica, si alguna vez no está seguro de si un cliente ha decidido trabajar con usted, debe contactar con él. Adicionalmente, puede obtener el consentimiento por vía electrónica (por ejemplo, por correo electrónico o mensaje de texto) o en persona.
- » Los documentos de consentimiento deberán estar debidamente protegidos y conservarse durante 10 años.
- » El consentimiento debe reconocer que el agente o corredor ha informado al consumidor de las funciones y responsabilidades que se aplican al papel del agente o corredor en el Mercado.
- » Si los agentes o corredores venden o transfieren su libro de negocios a otro productor, deberán informar a los consumidores de los efectos de la venta y del cambio de NPN. Antes de trabajar con cualquier nuevo cliente, el nuevo agente o corredor está obligado a obtener el consentimiento del consumidor.

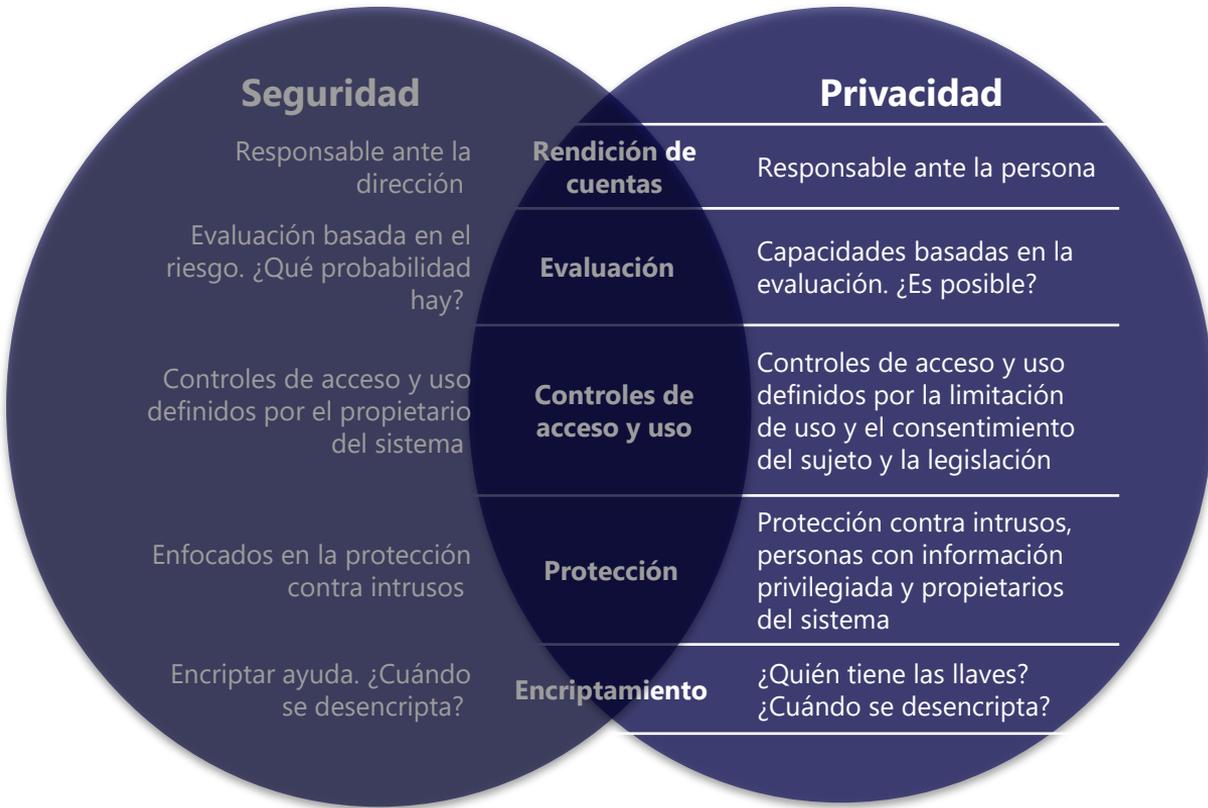
# ¿Qué es la seguridad de la información?



- » La seguridad de la información se refiere a la protección de la información y los sistemas de información contra el acceso, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados, con el fin de ofrecer:
  - Confidencialidad
  - Integridad
  - Disponibilidad
- » Un riesgo es el costo para el negocio en caso de que una vulneración sea explotada por una amenaza, causando daño a un activo.
  - Todos los sistemas de información tienen algún nivel de riesgo.
  - Los riesgos de seguridad de los sistemas de información suelen ser cualitativos, típicamente altos, moderados, bajos; y están relacionados con la confidencialidad, la integridad y la disponibilidad de la información y del sistema de información.

Gravedad del daño	Descripción
<b>Bajo</b>	Efecto adverso limitado: casi sin repercusiones, con poco costo, a un esfuerzo mínimo de reparación
<b>Moderado</b>	Efecto adverso grave: algún daño tangible, con un gasto moderado para reparar
<b>Alto</b>	Efecto adverso grave o catastrófico: daño a la reputación, pérdida de confianza, responsabilidad legal, interrupción considerable o prolongada, compromiso de la información, compromiso total de los servicios

La seguridad se refiere a los sistemas y las salvaguardias físicas que se utilizan para proteger la información personal de los consumidores.



La privacidad es el derecho del consumidor a controlar cómo se utiliza o divulga su información personal.

- » El Acuerdo de Privacidad y Seguridad del Mercado que usted ejecuta como parte del proceso de registro anual autoriza a los agentes y corredores a crear, recopilar, divulgar, acceder, mantener, almacenar y utilizar datos específicos y PII. Los agentes y corredores no pueden divulgar, publicar o revelar la PII del consumidor a personal no autorizado, y deben proteger esta información de acuerdo con las leyes y reglamentos federales relativos al manejo de la PII.
- » La PII se refiere a la información que puede usarse para distinguir o rastrear la identidad de un individuo, como su nombre, número del seguro social, registros biométricos, etc. por sí solos, o cuando se combinan con otra información personal o de identificación que está vinculada o es vinculable a un individuo específico.<sup>1</sup>
- » Debe brindar a los consumidores la posibilidad de optar y utilizar su PII (y la de su agencia, de ser el caso) (por ejemplo, mediante el registro de consentimiento). También debe aportar un mecanismo a través del cual el consumidor, o su representante autorizado, pueda limitar el uso de su PII.

<sup>1</sup>Esta definición de PII fue tomada de la Política de Privacidad de CMS.gov disponible en <https://www.cms.gov/privacy>.

Hay diversos tipos de PII. PII es toda la información que su organización clasifica como sensible, como por ejemplo:

- » Domicilio del solicitante +
- » Importe máximo del APTC del solicitante
- » Nivel de CSR de los solicitantes
- » Ingresos de la Vivienda del solicitante
- » ID del solicitante de los intercambios facilitados por el gobierno federal (FFE)
- » Cuenta corriente y número de registro

## Otros tipos de información protegida son: +

- » Información médica protegida (PHI), como historiales médicos y resultados de laboratorio
- » Información fiscal federal

# Cómo proteger la PII de los consumidores



- » Como agente o corredor, puede proteger la PII de los consumidores:
  - Aplicar el principio de "necesidad de saber" antes de revelar la PII a otras personas.
  - Evaluar una necesidad de PII requerida antes de compartir otras
  - Limitación de la PII al uso oficial



- » Los agentes y corredores también están obligados a capacitar y supervisar a su personal sobre los requisitos relacionados con el uso autorizado y el intercambio de PII con terceros, y las consecuencias del uso no autorizado o el intercambio de PII, y a auditar periódicamente su uso real y la divulgación de PII.<sup>1</sup>

<sup>1</sup> Esta información está tomada del Acuerdo de Privacidad y Seguridad del Mercado Individual para el Año Planeado 2022, Sección II, Párrafo E "Duty to Protect PII."

# Verificación de conocimientos #1

Kelly está trabajando en un informe sobre un cliente dirigido a su gerente. Para Kelly es más rápido extraer los datos de los clientes existentes de otro informe que crear uno nuevo. El informe existente también contiene números del seguro social y fechas de nacimiento, información que Kelly no requiere. ¿Está bien que Kelly utilice el informe y así ahorrar tiempo?



a) Sí, porque le ayudará a hacer su trabajo.

b) No, los agentes y corredores sólo deben acceder a la información en la medida en que sea necesario para desempeñar su función laboral y únicamente para fines autorizados.



## Personalmente

- » Guarde los formularios de consentimiento del consumidor impresos en un lugar cerrado con llave.
- » Durante las citas con los consumidores, utilice espacios reservados para garantizar la privacidad.
- » Eliminar la PII de forma coherente con las normas de FFM y los requisitos de conservación.



## De manera electrónica

- » No envíe ni reenvíe correos electrónicos con PII a cuentas de correo electrónico personales.
- » No utilice dispositivos móviles no autorizados para acceder a la PII.
- » Guarde la PII de forma segura en un archivo protegido con contraseña en una computadora protegida con contraseña a la que sólo tengan acceso las personas autorizadas.



## En Papel

- » Asegúrese de que los registros originales de los consumidores sean devueltos antes de que sean retirados de su oficina y sólo haga copias para usted o para otras personas, si fuese necesario, para llevar a cabo las tareas requeridas.
- » Conserve una reserva de carpetas de papel manila para entregar los documentos de los consumidores, a fin de mantenerlos en un solo lugar y proteger el contenido para que no sea visto.

¿Qué significa proteger la PII al limitar el uso autorizado e intercambio de PII con terceros?



- a) Los agentes y corredores deberán aplicar el principio de necesidad de conocer cuando se trate del uso autorizado de la PII, y si los agentes o corredores venden o transfieren su libro de negocios a otro proveedor, deberán informar a los consumidores afectados por la venta y el cambio de NPN.
- b) Los agentes y corredores no deben compartir la PII con nadie bajo ninguna circunstancia.
- c) Los agentes y corredores pueden compartir la PII con cualquier persona de su organización, siempre y cuando no se comparta con nadie fuera de la organización.
- d) Los agentes y corredores no pueden compartir la PII con nadie de su empresa, incluso si eso supone ayudar al consumidor con las funciones de inscripción necesarias.

# Suspensión por riesgo para las operaciones o sistemas del Mercado



- » Los CMS pueden suspender inmediatamente la capacidad de un agente o corredor para acceder a los sistemas del Mercado, si descubren circunstancias que suponen un riesgo inaceptable para las operaciones del Mercado, o los sistemas de tecnología de la información, hasta que el incidente o la vulneración se solucione o se mitigue lo suficiente a entera satisfacción del HHS.
  - La implementación de esta disposición suspendería el acceso de un agente o corredor al Portal Enterprise de CMS, al Sistema de Gestión de Aprendizaje del Mercado (MLMS) y a las vías clásicas de DE/EDE.
  - La rescisión en virtud de lo dispuesto en la norma 45 C.F.R. § 155.220(g)(5) incluirá un aviso previo de 30 días, en el que los agentes tendrán la oportunidad de presentar pruebas para refutar las conclusiones de los CMS antes de la rescisión.
- » Si alguna vez se suspende su acceso al Mercado y tiene preguntas sobre ello, póngase en contacto con el servicio de asistencia para agentes/corredores: [FFMProducer-AssisterHelpDesk@cms.hhs.gov](mailto:FFMProducer-AssisterHelpDesk@cms.hhs.gov)

# Vulneración de la ciberseguridad



- » Las vulneraciones a la ciberseguridad son una amenaza creciente para las pequeñas empresas.
- » Los pequeños negocios son el blanco porque tienen información que los hackers quieren, y a menudo carecen de la infraestructura de seguridad de las grandes empresas.
- » El 88% de los propietarios de pequeños negocios considera que su empresa es vulnerable a un ciberataque, según una reciente encuesta de la Oficina para la Administración de Pequeños Negocios. Sin embargo, muchas empresas no saben por dónde empezar cuando se trata de ciberseguridad.

- » Una vulneración es la pérdida de control, el compromiso, la divulgación no autorizada, la adquisición no autorizada, el acceso no autorizado o cualquier otro término similar que se refiera a situaciones en las que personas distintas de los usuarios autorizados y con fines distintos a los autorizados tengan acceso o puedan tener acceso a información personal identificable, ya sea física o electrónica.<sup>1</sup>

## **Algunos ejemplos comunes de vulneraciones son:**

- Se pierde o se roba una laptop o un dispositivo de almacenamiento portátil que almacena PII;
- Se envía por error un correo electrónico o una carta que contiene PII, a quien no corresponde; o
- Un usuario autorizado accede o utiliza la PII para un propósito no permitido.

- » Un incidente es un evento o acción adversa no planificada, inusual y no deseada, que ha ocurrido como resultado del incumplimiento de las políticas y procedimientos de privacidad de la empresa. Debe referirse al uso o divulgación no autorizados de la PII, incluida la "divulgación accidental", como los correos electrónicos o faxes con dirección errónea<sup>1</sup>.

<sup>1</sup>Estas definiciones están tomadas del Memorandum 17-12 de la Oficina de Administración y Presupuesto (OMB), disponible en [https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12\\_0.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf).

- » Un incidente de seguridad es un evento notificable que cumple uno o más de los siguientes criterios:
  - El acceso, el uso, la divulgación, la modificación o la destrucción no autorizados de información o la interferencia con las operaciones en un sistema de información.
  - La pérdida de datos por robo, extravío de dispositivos, extravío de documentos impresos y desvío de correo electrónico.
  - Un evento que pone en peligro real o potencialmente la confidencialidad, integridad y disponibilidad de un sistema de información o de la información.
  - Una vulneración o amenaza de vulneración de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.

## Las amenazas comunes incluyen:

- Ingeniería social
- Phishing (suplantación de identidad)
- Malware (Viruses, ransomware, etc.)
- Parches inadecuados o pospuestos

- » Robo de una computadora portátil, una unidad de memoria o un disco duro portátil que contenga PII encriptada o sin encriptar +
- » Enviar documentos impresos que contengan PII a una dirección incorrecta,
- » Acceso no autorizado a los expedientes personales o médicos
- » Envío de correos electrónicos con información médica, desde una cuenta de correo electrónico de la empresa a una cuenta de correo electrónico personal
- » Un hacker accede a una computadora y a sus cuentas
- » Dejando los documentos que contienen PII al descubierto, en una zona en la que personas sin acceso autorizado pudieran leerlos, copiarlos o transferirlos para su uso futuro.

- » La "ingeniería social" intenta manipularlo para que divulgue involuntariamente información a un hacker, o para que realice una acción que conduzca a una vulneración de la seguridad o la privacidad.
- » Los hackers pueden hacerse pasar por un compañero de trabajo o un "amigo" en un esfuerzo por ganarse su confianza para poder obtener acceso a su información y sistemas de información.
- » Los hackers también pueden acechar las redes Wi-Fi gratuitas, como las de las cafeterías, los aeropuertos y los hoteles.

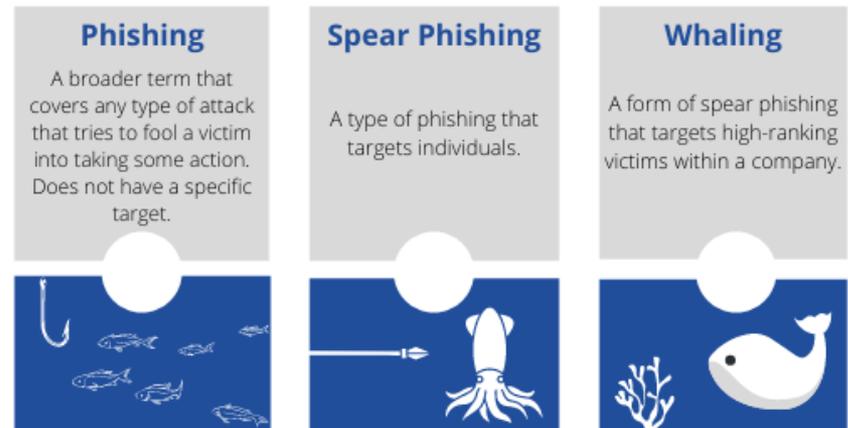
## **La ingeniería social consiste en:**

- » Sitios web de apariencia normal que parecieran ser legítimos, pueden estar conectados con enlaces maliciosos o malware que infectan los dispositivos de los visitantes.
- » Las "solicitudes de amistad" en las redes sociales pueden hacerse pasar por amigos y colegas para engañarle y hacerle aceptar programas maliciosos o divulgar información sensible.

# Amenazas comunes: Phishing (suplantación de identidad)

- » El phishing es una forma de ingeniería social mediante la cual los intrusos tratan de obtener acceso a la información y a los sistemas de información haciéndose pasar por una persona, empresa u organización real con motivos legítimos para solicitar la información.
  - » Los correos electrónicos (o textos) de phishing suelen alertar al usuario de un problema con su cuenta y le piden que haga clic en un enlace para aportar información que corrija el problema.
- 
- » Estos enlaces pueden descargar programas maliciosos en su computadora o dispositivo móvil y permitir que el atacante acceda al dispositivo, a los dispositivos conectados y a la información almacenada en esos dispositivos.
  - » Estos correos electrónicos suelen tener un aspecto real y parecen contener logotipos y marcas comerciales reales. Pueden estar dirigidos personalmente a usted y parecer enviados por una fuente legítima que usted conoce y en la que confía, como una dependencia gubernamental o una entidad comercial.
  - » La URL aportada puede incluso parecerse a la dirección web auténtica, por ejemplo, "Amazons.com" con un error ortográfico muy pequeño que se podría pasar por alto fácilmente.

## Phishing vs. Spear Phishing vs. Whaling



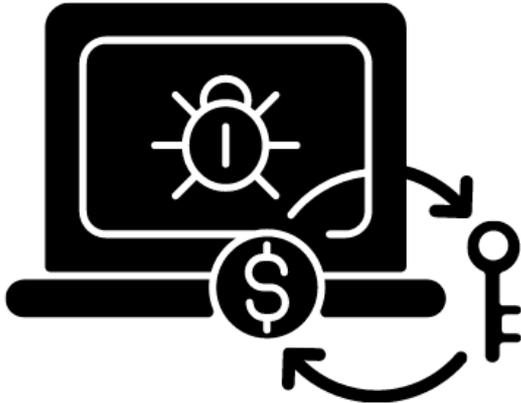
# Amenazas comunes: Malware



- » El malware (abreviatura de software malicioso) daña, roba información o interrumpe un sistema informático.
- » El malware suele instalarse a través de un usuario:
  - Abrir archivos adjuntos infectados en el correo electrónico
  - Descargar archivos infectados
  - Visitar una página web infectada
- » El malware (incluido el ransomware) puede corromper archivos, borrar el disco duro o dar a un hacker el control de su ordenador.
- » Protéjase del malware:
  - Lea los correos electrónicos en texto plano.
  - Examine los archivos adjuntos con un software antivirus antes de descargarlos. Nunca abra un archivo adjunto de alguien que no conoce.
  - Utilice el botón Spam para denunciar los correos electrónicos sospechosos sin necesidad de abrirlos.
  - Si cree que la computadora de su empresa, que contiene información delicada del Mercado, está infectada, póngase en contacto con el servicio de asistencia informática de CMS en [CMS IT Service Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov)

# Amenazas comunes: Ransomware

- » El ransomware es un tipo de malware que infecta y restringe el acceso a una computadora, encriptando los archivos y dejándolos inutilizables, así como los sistemas que dependen de ellos.
- » Los hackers exigen entonces el pago de un rescate a cambio del descriptamiento.



## El ransomware aparece en distintas formas:

- » Correos electrónicos de phishing
- » Aprovecha las vulneraciones no corregidas en el software

- » **Los agentes y corredores deben seguir medidas de precaución de "higiene de ciberseguridad" para mantener seguros los datos sensibles de los clientes y protegerlos de robos y ataques.**
- » La higiene de la ciberseguridad es un conjunto de prácticas que deben realizarse regularmente para mantener la seguridad de los dispositivos y redes.
- » **¿Qué se puede hacer?**
  - Aprender más sobre las amenazas cibernéticas más comunes
  - Comprender dónde es vulnerable su empresa
  - Tomar medidas para mejorar la ciberseguridad

Las prácticas de higiene en ciberseguridad incluyen:

- » **Respaldo:** Realice regularmente copias de seguridad de los archivos importantes en una ubicación separada y segura que permanezca a salvo en caso de fallo de ciberseguridad.
- » **Conciencia y educación:** Aprenda a evitar las estafas de phishing y a prevenir los ataques de malware. Los agentes y corredores también deben compartir esta información con sus empleados.
- » **Encriptamiento:** Utilice la encriptación para proteger los datos sensibles en los archivos y en los dispositivos.

- » Las mejores prácticas de higiene de ciberseguridad también incluyen:
  - **Higiene en las contraseñas:** Mantenga una buena higiene de las contraseñas exigiendo contraseñas únicas, empleando gestores de contraseñas, revisando la frecuencia de los ciclos y utilizando la autenticación multifactorial (MFA) cuando sea posible para dificultar el acceso no autorizado de los hackers.
  - **Gestión de parches:** Mantenga siempre el software actualizado e instale los parches de seguridad tanto en los dispositivos propiedad de la empresa como en los personales utilizados para el trabajo.
  - **Software de seguridad:** Instale software de seguridad para defender los sistemas contra programas maliciosos como ransomware, spyware, gusanos, rootkits y troyanos. Asimismo, ejecute escaneos regulares para detectar actividades inusuales.

# Verificación de conocimientos #3

Dan ha recibido un correo electrónico dirigido personalmente a él y que parece enviado por una fuente legítima que conoce y en la que confía. El correo electrónico le notifica que hay un problema con su cuenta y le pide que haga clic en un enlace para que brinde información y corregir el problema. Dan no era consciente de que hubiera un problema con su cuenta y duda en hacer clic en el enlace. También se da cuenta de que la URL aportada se parece a una dirección web auténtica, pero tiene un pequeño error ortográfico, por ejemplo, "Googlle.com". ¿Qué debería hacer? **Seleccione las opciones que correspondan.**



- a) Hacer clic en el enlace y aportar información para corregir el problema con su cuenta.
- b) Verificar con su departamento de informática para asegurarse de que el correo electrónico sea legítimo.
- c) No hacer clic en el correo electrónico y eliminar el mensaje.
- d) Reenvía el correo electrónico a su colega y pregunta si el correo es auténtico.

# Verificación de conocimientos #4

Taylor está de viaje y el hotel en el que se aloja ofrece Wi-Fi gratuito. ¿Está bien que ella utilice esta Wi-Fi para acceder a su correo electrónico de trabajo y a sus archivos de trabajo protegidos?



- a) No, conectarse a redes Wi-Fi gratuitas e inseguras puede exponer su ordenador a riesgos de seguridad innecesarios.
- b) Sí, el hotel no ofrecería Wi-Fi gratuito si no fuera seguro utilizarlo.
- c) Sí, ella sólo se conectará al Wi-Fi durante un corto período de tiempo.

# Prevenir vulneraciones a la ciberseguridad

Los agentes y corredores deben seguir estos pasos para prevenir las vulneraciones a la ciberseguridad:



1  
Revisar la información aportada en este seminario web y otros recursos de privacidad y seguridad de los CMS.

2  
Identificar los tipos de información a los que su empresa accederá, procesará, almacenará o transmitirá.

3  
Identificar el acceso de los usuarios, la solidez de las contraseñas y los procedimientos de seguridad para todos los sistemas.

4  
Después de evaluar los riesgos potenciales, establezca límites que protejan la PII y otra información sensible.

5  
Implemente restricciones apropiadas para su negocio.

Los agentes y corredores deben seguir las fases de respuesta a la vulneración de la seguridad y a los incidentes y documentar cada paso para su resolución



## Saber cómo actuar durante un incidente: +

- » Ayuda a resolver el problema con eficiencia
- » Minimizar la pérdida de información
- » Minimizar la interrupción de los servicios, o las vulneraciones de la seguridad

# Informar sobre vulneración de la ciberseguridad



## En caso de duda, ¡informe!

- » Todas las vulneraciones e incidentes potenciales y confirmados deben ser comunicados a los CMS. Si no está seguro de si se trata de una vulneración, de un incidente o no tiene nada que ver, es mejor denunciarlo.
- » No espere a terminar las investigaciones internas para informar de una vulneración o incidente.
- » Tomamos en cuenta los esfuerzos de "buena fe" para notificar un incidente a tiempo, pero los plazos de notificación están establecidos para garantizar la seguridad del consumidor.

- » El acuerdo de privacidad y seguridad del agente corredor individual del Mercado y el acuerdo de SHOP del agente corredor requieren lo siguiente:
  - Exigir que se informe de cualquier vulneración de la PII al servicio de asistencia informática de los CMS por teléfono al (410) 786-2580 o al 1-800-562-1963 o mediante notificación por correo electrónico a [CMS IT Service Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov) en un plazo de 24 horas desde el conocimiento de la vulneración. Los incidentes deberán notificarse al servicio de asistencia informática de la CMS utilizando los mismos medios que las vulneraciones en un plazo de 72 horas desde el conocimiento del incidente. Notificar una vulneración o un incidente no significa admitir que se ha cometido un error.

Si usted es un agente o corredor que utiliza los sitios asociados de DE o EDE para sus inscripciones, y considera que otra persona ha utilizado su cuenta o ha accedido a ella, debe informar inmediatamente del incidente al servicio de asistencia de TI de los CMS ([CMS IT Service Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov)) y al servicio de asistencia para agentes corredores del sitio web asociado de DE/EDE. Por favor, asegúrese también de actualizar sus contraseñas para acceder a su cuenta DE/EDE lo antes posible.

- » Cuando se ponga en contacto con el servicio de asistencia informática de los CMS por correo electrónico en relación con una vulneración o un incidente de seguridad, una buena práctica sería presentar un informe de incidentes de seguridad (SIR). La plantilla del SIR (informe de incidentes de seguridad) puede encontrarse en.
  - <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template>
- » Después de informar:
  - El Equipo de Gestión de Incidentes (IMT) emitirá un número de incidente para su seguimiento.
  - El IMT derivará a los equipos apropiados que son responsables del seguimiento y la investigación.
  - Si tiene información adicional que proporcionar con respecto a su informe de incidente, puede aportar actualizaciones llamando o enviando un correo electrónico a los servicios de asistencia de TI de CMS. Por favor, informe que usted está aportando una actualización y utilice el número de incidente que se emitió cuando usted informó originalmente.

- » [CMS Information Security and Privacy Library](#) es un recurso que aporta información adicional sobre cómo los CMS llevan a cabo la ciberseguridad.
- » [CISA's Cyber Essentials](#) sirve de guía para que los pequeños negocios sepan por dónde empezar a aplicar las prácticas de ciberseguridad.
- » La Oficina de Administración para los Pequeños Negocios ofrece sesiones de capacitación gratuitas sobre ciberseguridad. Inscríbase en sus capacitaciones [aquí](#).
- » La [Alianza Nacional de Ciberseguridad](#) también ofrece [eventos virtuales y presenciales sobre ciberseguridad](#) para ayudar a los propietarios de pequeños negocios a informarse sobre la ciberseguridad y cómo mantenerse seguros.
- » Para mayor información sobre el cumplimiento de las normas en el Mercado, consulte [Cumplimiento de los requisitos del Mercado: Diapositivas del seminario web para agentes y corredores](#).

¿Cómo puedo identificar y notificar una vulneración de la ciberseguridad?



- a) Esperar hasta estar seguro de que se trata de una vulneración de la ciberseguridad y entonces llamar a la policía.
- b) Intentando resolver el problema por sí mismo y no denunciarlo.
- c) Intentando resolver el problema usted mismo, y si no es capaz, contactando con el servicio de asistencia informática de los CMS.
- d) Aprendiendo por sí mismo a identificar las vulneraciones de la ciberseguridad y poniéndose en contacto con el servicio de asistencia informática de los CMS en un plazo de 24 horas en caso de que se produzca un problema.

¿Cómo puedo mantener un nivel de seguridad que sea coherente con los requisitos de cumplimiento de los CMS y que ofrezca la máxima protección a mis clientes y a mi empresa?



- a) Revisando el acuerdo de privacidad y seguridad de los CMS y el acuerdo de agente corredor de 2022 para garantizar el cumplimiento y aplicar los controles de seguridad adecuados.
- b) Revisando el acuerdo de privacidad y seguridad de los CMS y el acuerdo de agente corredor de 2022 y luego implementar controles de máxima seguridad en todos los dispositivos.
- c) Mediante la búsqueda de otra capacitación en línea sobre ciberseguridad y utilizar esos requisitos para actualizar los controles y dispositivos del sistema.
- d) Preguntando a los clientes con qué nivel de seguridad se sienten más cómodos.

¿Por qué es importante acceder sólo a la cantidad mínima de recursos e información necesaria para realizar las funciones de inscripción?



- a) Porque el acceso a la información sensible debe estar al alcance de todos.
- b) Porque el acceso a la información sensible sólo debe concederse para las funciones de inscripción necesarias.
- c) Porque el acceso a la información sensible no debe estar disponible para nadie más que para el agente o corredor que trabaja con el consumidor.
- d) Porque el acceso a la información sensible sólo debe concederse a las personas de su organización.

# Servicios de asistencia y centros de atención telefónica para agentes/corredores del Mercado



Nombre	# de teléfono y/o dirección de correo electrónico	Tipos de consultas atendidas	Horario (Cerrado los días festivos)
Servicio de asistencia del Mercado	1-855-CMS-1515 1-855-267-1515	<ul style="list-style-type: none"> <li>Restablecimiento de contraseñas y bloqueo de cuentas en el Portal Enterprise de CMS</li> <li>Otros problemas o mensajes de error de la cuenta del portal Enterprise de CMS</li> <li>Preguntas generales sobre el registro y la capacitación (no relacionadas con una plataforma de formación específica)</li> <li>Problemas de inicio de sesión en la página de inicio de inscripción directa del agente/corredor</li> <li>Problemas técnicos o específicos del sistema relacionados con el MLMS</li> <li>Preguntas específicas de los usuarios sobre la navegación en el sitio MLMS o el acceso a la capacitación y los exámenes</li> </ul>	Lunes-Viernes 8:00 AM-8:00 PM ET Solo en octubre-noviembre Sábado y domingo, de 10:00 a 15:00 ET
Servicio de asistencia por correo electrónico para agentes/corredores	FFMProducer-AssisterHelpDesk@ <a href="mailto:cms.hhs.gov">cms.hhs.gov</a>	<ul style="list-style-type: none"> <li>Preguntas generales sobre la inscripción y la compensación</li> <li>Comprobación manual de la identidad/problemas con Experian</li> <li>Preguntas generales escaladas sobre el registro y la capacitación (no relacionadas con una plataforma de formación específica)</li> <li>Problemas de RCL de agentes/corredores</li> <li>Listado de temas de Find Local Help (Encontrar Ayuda local)</li> <li>Instrucciones o preguntas sobre la participación en Help On Demand</li> <li>Reportar preocupaciones de que un consumidor u otro agente o corredor hayan incurrido en fraude o conducta abusiva</li> </ul>	Lunes-Viernes 8:00 AM-6:00 PM ET
Línea de Atención Telefónica de socios de agentes/corredores del Mercado	1-855-788-6275 Nota: Ingrese su NPN para tener acceso a este número. Usuarios de TTY 1-855-889-4325	Preguntas específicas de las solicitudes de los consumidores relacionadas con: <ul style="list-style-type: none"> <li>Restablecimiento de contraseña para una cuenta de HealthCare.gov de un consumidor,</li> <li>Opciones de inscripción especiales (SEP) no disponible en la solicitud del consumidor,</li> <li>Preguntas específicas de los consumidores sobre la elegibilidad y la inscripción</li> </ul>	Lunes a domingo 24 horas/día
Servicio de atención al cliente de TI de los CMS	(410) 786-2580 o al 1-800-562-1963 <a href="mailto:CMS.IT.Service.Desk@cms.hhs.gov">CMS.IT.Service.Desk@cms.hhs.gov</a>	<ul style="list-style-type: none"> <li>Informar de una vulneración a la seguridad o de un incidente</li> </ul>	Lunes-Viernes 9:00 AM-5:00 PM ET

# Definiciones de siglas



Sigla	Definición
CCIIO	Centro de Información al Consumidor y Supervisión de Seguros
CMS	Centros de Servicios de Medicare y Medicaid
DE	Inscripción directa
DHS	Departamento de Seguridad Nacional
EDE	Inscripción directa mejorada
FTI	Información fiscal federal
HIPAA	Ley de Portabilidad y Responsabilidad de Seguros Médicos
HITECH	Ley de Tecnologías de la Información Económica y Clínica de la Salud

Sigla	Definición
IMT	Equipo de gestión de incidentes
OMB	Oficina de Administración y Presupuesto
PII	Información personal identificable
PHI	Información médica protegida
PPACA/ACA	Ley de Cuidado de Salud a Bajo Precio de Protección al Paciente
SIR	Informe de incidentes de seguridad
SSN	Número del Seguro Social